

## POC Radius, rapport mise en service

### Table des matières

POC Radius, rapport mise en service .....	1
User Story 1 .....	1
Test d'acceptation : .....	1
User Story 2 .....	2
Test d'acceptation : .....	3
User Story 3 .....	5
Test d'acceptation : .....	5

### User Story 7

En tant que responsable de la sécurité, je veux qu'uniquement les flux identifiés (dans l'exercice précédent sur la DMZ ainsi que les nouveaux flux identifiés dans cet exercice) soit autorisé à traverser le routeur, dans le but de protéger l'infrastructure d'accès non autorisés. Dessiner les divers flux sur le schéma

Tests d'acceptation :

Schéma des flux et tableau des actions

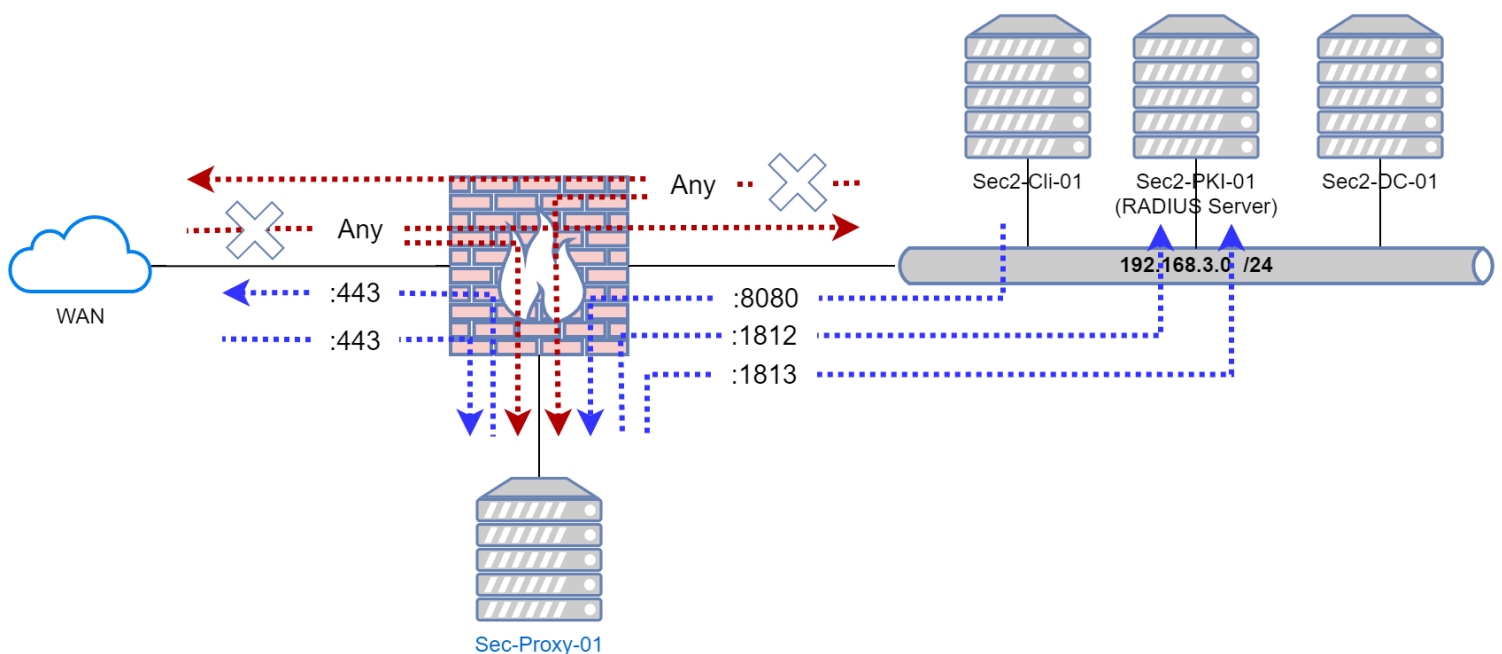


Tableau des actions :

## Voir Tableau dans Regles Rapport 1

*Image avec les règles du firewall, (onglet Filter Rules de IP Firewall sur Winbox), mettez des commentaires dans les règles afin d'éclaircir la lecture*

## Voir images dans Regles Rapport 1

### User Story 8

En tant que responsable de la sécurité, je veux que l'ensemble de mon routeur (Mikrotik) puisse être consulté en lecture seul par les utilisateurs du groupe secu\_net\_admin par l'utilisation d'un protocole AAA, dans le but d'accroître la sécurité et la granularité des accès.

Valeur «Class» reçue du serveur RADIUS

Cette valeur devrait correspondre à un groupe OPNsense

Dans mon cas la valeur est paramétrée à «NetAdmins»

# Client Radius Opnsense

System: Access: Servers	
<b>Descriptive name</b>	Radius Server
<b>Type</b>	Radius
<b>Hostname or IP address</b>	<input type="text" value="192.168.3.11"/>
<b>Shared Secret</b>	<input type="password" value="....."/>
<b>Services offered</b>	<div>Authentication and Accounting</div>
<b>Authentication port value</b>	<input type="text" value="1812"/>
<b>Accounting port value</b>	<input type="text" value="1813"/>
<b>Authentication Timeout</b>	<input type="text" value="5"/>
<b>Synchronize groups</b>	<input checked="" type="checkbox"/>
<b>Limit groups</b>	<div>NetAdmins</div>
<b>Automatic user creation</b>	<input type="checkbox"/>
<b>Protocol</b>	<div>MSCHAPv2</div>
<div>Save</div>	

Propriétés de sec2-dmz-01

Paramètres

Avancé

☒ Activer ce client RADIUS

☐ Sélectionner un modèle existant :

Nom et adresse

Nom convivial :

sec2-dmz-01

Adresse (IP ou DNS) :

192.168.3.1

Vérifier...

Secret partagé

Sélectionnez un modèle de secrets partagés existant :

Aucun

Pour taper manuellement un secret partagé, cliquez sur Manuel. Pour générer automatiquement un secret partagé, cliquez sur Générer. Vous devez configurer le client RADIUS avec le même secret partagé entré ici. Les secrets partagés respectent la casse.

☒ Manuel☐ Générer

Secret partagé :

.....

Confirmez le secret partagé :

.....

OK

Annuler

Appliquer

# Radius Server NPS Policy

**Stratégies réseau**

Les stratégies réseau

Nom de la stratégie

- access\_PROXY
- OPNsense\_Access
- Connexions de réseau pri
- Connexions à d'autres se
- Connexions au serveur M

OPNsense\_Access

Conditions - Si les conditio

Condition

- Nom convivial du client
- Groupes Windows

Paramètres - Les paramètr

Paramètre

- Méthode d'authentificatio
- Autorisation d'accès
- Framed-Protocol
- Service-Type
- Class

**Propriétés de OPNsense\_Access**

Vue d'ensemble Conditions Contraintes Paramètres

Nom de la stratégie : OPNsense\_Access

État de la stratégie

Si la stratégie est activée, le serveur NPS l'évalue lors de l'autorisation. Si elle est désactivée, le serveur NPS ne l'évalue pas.

☒ Stratégie activée

Autorisation d'accès

Si la demande de connexion répond aux conditions et contraintes de la stratégie réseau, celle-ci peut soit accorder l'accès, soit le refuser. [Qu'est-ce qu'une autorisation d'accès ?](#)

☒ Accorder l'accès. Accorder l'accès si la demande de connexion correspond à cette stratégie.

☐ Refuser l'accès. Refuser l'accès si la demande de connexion correspond à cette stratégie.

☐ Ignorer les propriétés de numérotation des comptes d'utilisateurs.

Si la demande de connexion répond aux conditions et contraintes de cette stratégie réseau, et si la stratégie accorde l'accès, l'autorisation est basée uniquement sur la stratégie réseau ; les propriétés de numérotation des comptes d'utilisateurs ne sont pas évaluées.

Méthode de connexion réseau

Sélectionnez le type de serveur d'accès réseau qui envoie la demande de connexion au serveur NPS. Vous pouvez sélectionner une valeur dans Type de serveur d'accès réseau ou bien Spécifique au fournisseur, mais ces paramètres ne sont pas obligatoires. Si votre serveur d'accès réseau est un commutateur d'authentification ou un point d'accès sans fil 802.1X, sélectionnez Non spécifié.

☒ Type de serveur d'accès réseau :

Non spécifié

☐ Spécifique au fournisseur :

10

OK Annuler Appliquer

**Propriétés de OPNsense\_Access**

Vue d'ensemble Conditions Contraintes Paramètres

Configurez les conditions de cette stratégie réseau.

Si la demande de connexion répond aux conditions, le serveur demande de connexion ne répond pas aux conditions, le serveur stratégies supplémentaires seraient configurées.

Condition	Valeur
Nom convivial du client	sec2-dmz-01
Groupes Windows	SECU03\NetAdmins

**Informations d'attribut**

Nom de l'attribut : Class

Numéro de l'attribut : 25

Format de l'attribut : OctetString

Entrez la valeur d'attribut dans :

☒ Chaîne

☐ Hexadécimal

NetAdmins

OK Annuler

# Connexion de test

System: Access: Tester

User: user2 authenticated successfully.  
This user is a member of these groups:

Attributes received from server:  
class => NetAdmins

Authentication Server

Radius Server

Username

user2

Password

••••••••

Test

## Log de la Connexion de test réussie

Propriétés de l'événement - Événement 6272, Microsoft Windows security auditing.

Général

Détails

Le serveur NPS a accordé l'accès à un utilisateur.

Utilisateur :

ID de sécurité :

SEC003\user2

Nom de compte :

user2@secu03.local

Domaine de compte :

SEC003

Nom de compte complet :

secu03.local/Users/user2

Ordinateur client :

ID de sécurité :

NULL SID

Nom de compte :

-

Nom de compte complet :

-

Identificateur de la station appelée :

-

Identificateur de la station appelante :

-

Serveur NAS :

Adresse IPv4 du serveur NAS :

-

Adresse IPv6 du serveur NAS :

-

Identificateur du serveur NAS :

65661a4e58f40

Type de port du serveur NAS :

Ethernet

Port du serveur NAS :

0

Client RADIUS :

Nom convivial du client :

sec2-dmz-01

Adresse IP du client :

192.168.3.1

Informations détaillées sur l'authentification :

Nom de stratégie de demande de connexion :

Proxy Access

Nom de stratégie réseau :

OPNsense\_Access

Fournisseur d'authentification :

Windows

Serveur d'authentification :

sec2-pki-01.secu03.local

Type d'authentification :

MS-CHAPv2

Type EAP :

-

Identificateur de la session du compte :

-

Résultats de la journalisation :

Les informations de suivi ont été inscrites dans le fichier journal local.

Journal :

Sécurité

Source :

Microsoft Windows security

Connecté :

28.11.2023 19:38:11

Événement :

6272

Catégorie :

Network Policy Server

Niveau :

Information

Mots-clés :

Succès de l'audit

Utilisateur :

N/A

Ordinateur :

sec2-pki-01.secu03.local

Opcode :

Informations

Informations :

[Aide sur le Journal](#)

## Propriétés de OPNsense\_Access

Vue d'ensemble Conditions Contraintes Paramètres






Configurez les contraintes de cette stratégie réseau.

Si la demande de connexion ne répond pas à toutes les contraintes, l'accès réseau est refusé.

Contraintes :

### Contraintes

#### Méthodes d'authentification

-  Délai d'inactivité
-  Délai d'expiration de session
-  ID de la station appelée
-  Restrictions relatives aux jours et aux heures
-  Type de port NAS

Autorisez l'accès uniquement aux clients qui s'authentifient à l'aide des méthodes spécifiées.

Les types de protocoles EAP sont négociés entre le serveur NPS et le client dans l'ordre dans lequel ils sont listés.

Types de protocoles EAP :

Monter

Descendre

Ajouter...

Modifier...

Supprimer

Méthodes d'authentification moins sécurisées :

- ☒ Authentification chiffrée Microsoft version 2 (MS-CHAP v2)
  - ☒ L'utilisateur peut modifier le mot de passe après son expiration
- ☒ Authentification chiffrée Microsoft (MS-CHAP)
  - ☒ L'utilisateur peut modifier le mot de passe après son expiration
- ☐ Authentification chiffrée (CHAP)
- ☐ Authentification non chiffrée (PAP, SPAP)
- ☐ Autoriser les clients à se connecter sans négocier une méthode d'authentification

## Propriétés de : user2

?

×

Environnement Sessions Contrôle à distance Profil des services Bureau à distance COM+  
Général Adresse Compte Profil Téléphones Organisation Membre de Appel entrant

Membre de :

Nom	Dossier Services de domaine Active Directory
admins	secu03.local/Users
NetAdmins	secu03.local/Users
Utilisateurs du do...	secu03.local/Users

Ajouter...

Supprimer

Groupe principal : Utilisateurs du domaine

Définir le groupe principal

Il n'est pas utile de modifier le groupe principal, sauf si vous disposez de clients Macintosh ou d'applications compatibles POSIX.

OK

Annuler

Appliquer

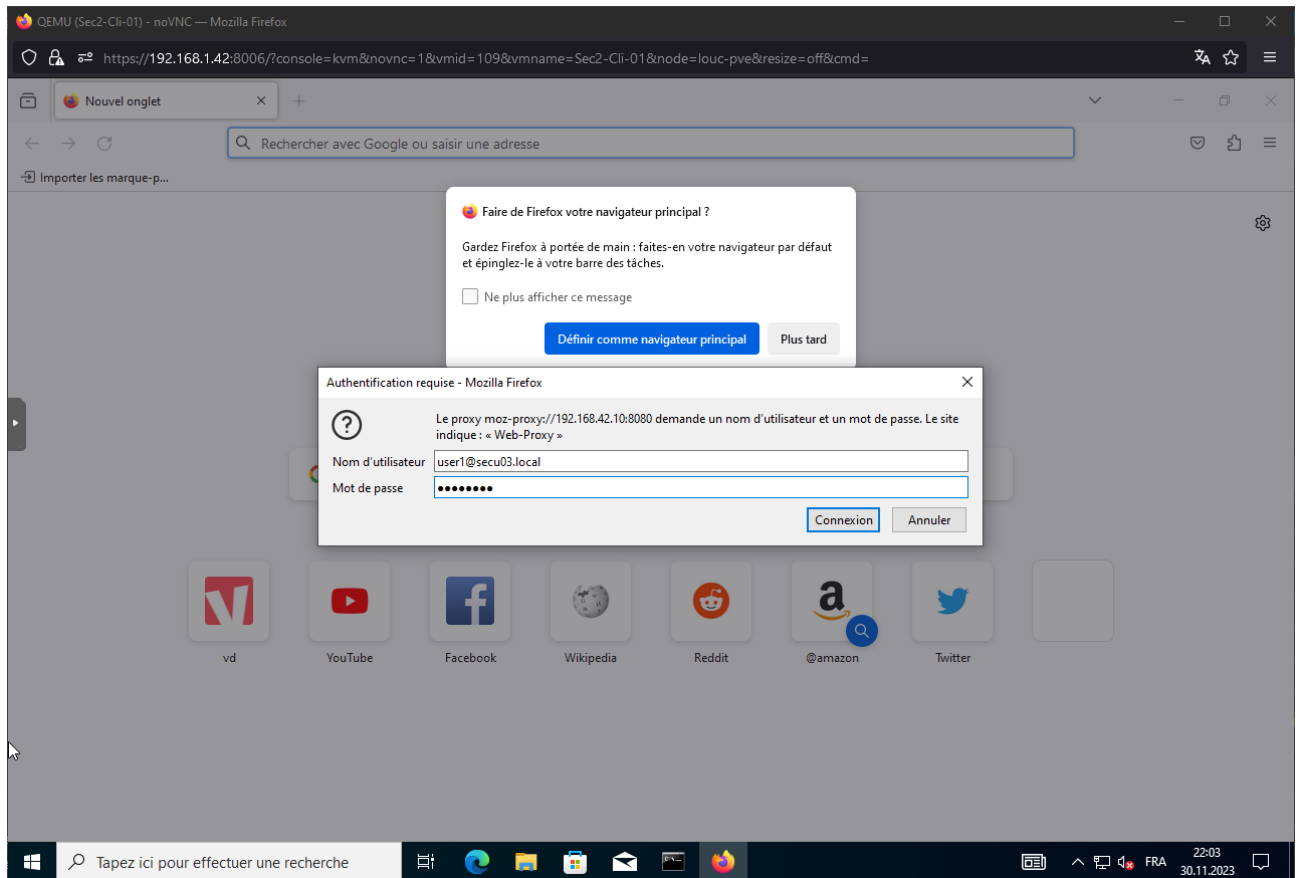
Aide

## User Story 9

En tant que responsable de la sécurité, je veux que l'ensemble des utilisateurs du domaine puissent surfer au travers du proxy de manière authentifiée par Radius, dans le but de répondre besoin de traçabilité des accès vers internet et d'obtenir des logs légaux à présenter en cas d'enquête.

### Tests d'acceptation :

Accès authentifié au proxy



Config du fichier /etc/squid/squid.conf

# Voir Tableau dans fichier de config Rapport 1

Nom de compte complet : secu03.local/Users/user1

Ordinateur client :

- ID de sécurité : NULL SID
- Nom de compte : -
- Nom de compte complet : -
- Identificateur de la station appelée : -
- Identificateur de la station appelante : -

Serveur NAS :

- Adresse IPv4 du serveur NAS : 192.168.42.10
- Adresse IPv6 du serveur NAS : -
- Identificateur du serveur NAS : -
- Type de port du serveur NAS : Asynchrone
- Port du serveur NAS : 111

Client RADIUS :

- Nom convivial du client : sec2-proxy-01
- Adresse IP du client : 192.168.42.10

Informations détaillées sur l'authentification :

- Nom de stratégie de demande de connexion : Proxy Access
- Nom de stratégie réseau : access\_PROXY
- Fournisseur d'authentification : Windows
- Serveur d'authentification : sec2-pki-01.secu03.local
- Type d'authentification : PAP
- Type EAP : -
- Identificateur de la session du compte : -
- Résultats de la journalisation : Les informations de suivi ont été inscrites dans le fichier journal local.

Journal : Sécurité

Source : Microsoft Windows security Connecté : 30.11.2023 22:04:32

Événement : 6272 Catégorie : Network Policy Server

Niveau : Information Mots-clés : Succès de l'audit

Utilisateur : N/A Ordinateur : sec2-pki-01.secu03.local

Opcode : Informations

Informations : [Aide sur le Journal](#)

## Log legaux

```
1701378440.923 8 192.168.3.50 TCP_DENIED/403 4474 POST http://ocsp.swisssign.net/DA340498E1013F46A208CB41FF32811DE5E01C40E user1@secu03.local HIER_NONE/- text/html
1701378440.947 71 192.168.3.50 TCP_TUNNEL/200 8981 CONNECT prestations.vd.ch:443 user1@secu03.local HIER_DIRECT/145.232.192.146 -
1701378445.332 5079 192.168.3.50 TCP_TUNNEL/200 8492 CONNECT vd.ch:443 user1@secu03.local HIER_DIRECT/145.232.192.197 -
```

Conclusion concernant l'authentification Radius du navigateur par le proxy

Deux fonctions différentes du protocole RADIUS sont utilisées :

### Authentication

Pour la Policy Proxy Access qui authentifie simplement l'utilisateur

### Accounting

Pour la Policy OPNsense\_Access qui envoie des informations d'appartenance à des groupes utilisateurs en vue d'attribution de droits spécifique sur le client RADIUS